Chapter 11

Configuring Dynamic IP Tunnels

IP tunnels provide a way of transporting datagrams between routers separated by networks that do not support all the protocols that those routers support. This chapter describes how to configure dynamic IP tunnels on E-series routers; it contains the following sections:

Dynamic IP Tunnel Overview

E-series routers support the following types of dynamic IP tunnels:

- Generic Routing Encapsulation (GRE) tunnels
- Distance Vector Multicast Routing Protocol (DVMRP) tunnels, also known as IP-in-IP tunnels

To establish a dynamic IP tunnel for GRE or DVMRP interfaces, you must configure a destination profile for a specific transport virtual router that is used to store tunnel configuration options, including the source and destination addresses of the dynamic IP tunnel.

A client application triggers the creation of dynamic IP tunnels based on the information stored in the GRE or DVMRP destination profile. The application specifies a tunnel source, tunnel destination, transport virtual router, and tunnel mode (GRE or DVMRP). If these parameters match those configured in the destination profile, the system creates the dynamic IP tunnel.

The application can automatically create an upper layer IPv4 interface over the GRE or DVMRP interface by using the IP characteristics defined in a profile referenced in the GRE or DVMRP destination profile.

Data MDT for Multicast VPNs and Dynamic IP Tunnels

The data multicast distribution tree (MDT) application for multicast VPNs can create dynamic point-to-multipoint GRE tunnels.

The data MDT application enables you to solve the problem of IP routers flooding unnecessary multicast information to PE routers that have no interested receivers for a particular VPN multicast group. The multicast data MDT solution requires the creation of a new dynamic IP tunnel by the PE router if the source exceeds a configured rate threshold parameter.

The data MDT application supports a co-located tunnel interface. The base GRE interface and its co-located data MDT interface must be both static or both dynamic.

The data MDT application creates a dynamic IP tunnel using the attributes in a customized destination profile.

When creating the dynamic IP tunnel, the data MDT application assigns its name using the following format:

mvpn-dynamic-*number*

For the data MDT application, you should configure a customized destination profile. For information about configuring multicast VPNs using GRE tunnels, see *JUNOSe Multicast Routing Configuration Guide, Chapter 3, Configuring PIM for IPv4 Multicast*.

Mobile IP and Dynamic IP Tunnels

The Mobile IP application can create dynamic point-to-point GRE and DVMRP tunnels.

The Mobile IP application is a tunneling-based solution that enhances the utility of E-series routing platforms at the edge of the network between fixed wire and wireless network domains. This tunneling-based solution enables a router on a user's home subnet to intercept and forward IP packets to users while they roam beyond traditional network boundaries.

To achieve mobility, the mobile node takes a secondary IP address that matches the new network and redirects the traffic bound to the primary or home address to the mobile node's new network. In the Mobile IP feature, the two agents that accomplish this task are the home agent and the foreign agent.

The Mobile IP application can create a dynamic IP tunnel using the attributes in a default destination profile or a customized destination profile.

When creating the dynamic IP tunnel, the Mobile IP application assigns its name using the following format:

mobileIp-dynamic-*number*

When the Mobile IP application creates the dynamic IP tunnel, it sets a Don't Fragment bit in the packet and in the outer IP header.

The Mobile IP home agent uses the dynamic IP tunnel for routing loop detection. The home agent examines packets that are intercepted by the home agent and destined for the mobile node. If the packet is already encapsulated, and the inner destination address is the same as the outer destination address, then the system examines the outer source address. If the outer source address is the same as the tunnel destination address or the foreign agent care-of-address (CoA), the system silently discards the packet. In all other cases, the tunnel encapsulation is successful.

For more information about configuring Mobile IP using GRE or DVMRP tunnels, see *Chapter 15, Configuring the Mobile IP Home Agent*.

Combining Dynamic and Static IP Tunnels in the Same Chassis

You can configure both dynamic and static IP tunnels in the same chassis.

A tunnel pair consists of two endpoints; one side encapsulates and the other side decapsulates. You can create a tunnel pair with two statically configured endpoints, two dynamically created endpoints, or with one static and one dynamic endpoint.

When configuring IP tunnels, you must consider that a tunnel is uniquely defined by its tunnel source, tunnel destination, transport virtual router, and mode (GRE or DVMRP). The system does not allow multiple tunnels with the same parameters. For example, when you configure a static tunnel with the same parameters as an existing dynamic IP tunnel, the system does not create the dynamic IP tunnel.

Changing and Removing Existing Dynamic IP Tunnels

You can modify the parameters in a destination profile referenced by existing dynamic IP tunnels. The changes only affect new dynamic IP tunnels that reference the destination profile.

You can relocate a dynamic IP tunnel for the Mobile IP application.

You cannot relocate a dynamic IP tunnel for the data MDT application because it is created using a profile. The system deletes dynamic IP tunnels that are relocated. Connections between a static tunnel endpoint and a dynamic tunnel endpoint can fail if the dynamic tunnel endpoint is deleted.

The client application removes dynamic IP tunnel interfaces when one of the following situations occur:

- The transport virtual router is removed.
- The tunnel interface relocates and the tunnel had an IP interfaced stacked on it.
- The tunnel interface indicates that setup is complete when the system is warm started, but it has no upper IP interface.

Platform Considerations

For information about modules that support IP tunnels on the ERX-7xx models, ERX-14xx models, and the ERX-310 router:

- See *ERX Module Guide, Table 1, Module Combinations* for detailed module specifications.
- See *ERX Module Guide, Appendix A, Module Protocol Support* for information about the modules that support IP tunnels.

For information about modules that support IP tunnels on the E120 router and the E320 router:

- See *E120 and E320 Module Guide, Table 1, Modules and IOAs* for detailed module specifications.
- See *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about the modules that support IP tunnels.

Module Requirements

The supported modules for creating IP tunnels depends on the type of E-series router that you have.

ERX-7xx Models, ERX-14xx Models, and the ERX-310 Router

To create dynamic IP tunnels on an ERX-7xx model, ERX-14xx model, or an ERX-310 router, you must install a Service line module (SM) or a module that supports the use of shared tunnel-server ports. For information about installing modules in the ERX routers, see the *ERX Hardware Guide*.

SMs provide dedicated tunnel-server ports that are always configured on the module. Unlike other line modules, SMs do not pair with corresponding I/O modules that contain ingress and egress ports. Instead, they receive data from and transmit data to other line modules with access to ingress and egress ports on their own associated I/O modules. However, you must assign interfaces on other line modules or loopback interfaces to act as source endpoints for the tunnel.

You can also create IP tunnels on router modules that support shared tunnel-server ports. You can configure (provision) a shared tunnel-server port to use a portion of the module's bandwidth to provide tunnel services. For a list of the modules that support shared tunnel-server ports, see the *ERX Module Guide*.

To configure IPSec transport mode in the GRE or DVMRP destination profile, you must install an IPSec Service Module (ISM).

For information about configuring tunnel services on dedicated and shared tunnel-server ports, see *JUNOSe Physical Layer Configuration Guide, Chapter 6, Managing Tunnel-Service and IPSec-Service Interfaces*.

All line modules forward traffic to IP tunnels. For information about which line modules accept traffic for IP tunnels, see the *ERX Module Guide*.

E120 Router and E320 Router

To create dynamic IP tunnels on an E120 router or an E320 router, you must install an ES2 4G line module (LM) with an ES2-S1 Service I/O adapter (IOA), or an IOA that supports the use of shared tunnel-server ports. For information about installing modules in these routers, see the *E120 and E320 Hardware Guide*.

The ES2 4G LM and ES2-S1 Service IOA combination provides a dedicated tunnel-server port that are always configured on the IOA. Unlike SMs, the ES2 4G LM requires the ES2-S1 Service IOA to condition it to receive and transmit data to other line modules. The ES2-S1 Service IOA also does not have ingress or egress ports.

You can also create IP tunnels on IOAs that support shared tunnel-server ports. You can configure (provision) a shared tunnel-server port to use a portion of the IOA's bandwidth to provide tunnel services. For a list of the IOAs that support shared tunnel-server ports, see the *E120 and E320 Module Guide*.

All line modules forward traffic to tunnels. For information about which IOAs accept traffic for tunnels, see the *E120 and E320 Module Guide*.

Redundancy and Tunnel Distribution

For information about the redundancy and tunnel distribution mechanisms supported for SMs, the ES2-S1 Service IOA, and shared tunnel-server ports, see *Tunnel-Service Interface Considerations* in *JUNOSe Physical Layer Configuration Guide, Chapter 11, Configuring Dynamic IP Tunnels*.

References

For more information about IP tunnels, see the following documents:

- RFC 1700—Assigned Numbers (October 1994)
- RFC 1701—Generic Routing Encapsulation (October 1994)
- RFC 1702—Generic Routing Encapsulation over IPv4 Networks (October 1994)
- RFC 2003—IP Encapsulation within IP (October 1996)
- RFC 2784—Generic Routing Encapsulation (GRE) (March 2000)

Configuring a Destination Profile for Dynamic IP Tunnels

The tasks in this section describe how to configure a destination profile for dynamic IP tunnels.

Modifying the Default Destination Profile

Default destination profiles for GRE and DVMRP are generated at system startup. The system supports only one default GRE destination profile and one default DVMRP destination profile.

The default destination profile enables the application to automatically create dynamic IP tunnels without user configuration for any virtual router, destination address, or source address.

By default, the data MDT application is disabled in the default destination profiles. The Mobile IP application can use the default destination profile. You can modify the configuration of the default destination profiles.

Modifying the Configuration of the Default Destination Profile

To modify the configuration in the default destination profile:

1. Specify the default destination profile for GRE or DVMRP.

   host1(config)#**gre destination profile global any-virtual-router**

2. Modify the options for the default destination profile.

   host1(config-dest-profile)#**tunnel mtu 5000**
   host1(config-dest-profile)#**tunnel checksum**

NOTE: You cannot configure a tunnel source, tunnel destination, or virtual router in the default destination profile.

Configuring a Destination Profile for GRE Tunnels

To configure a destination profile for dynamic GRE tunnels:

1. Configure a destination profile for GRE.

   host1(config-dest-profile)#**gre destination profile kanata1 virtual-router vr1**

2. Set the source address for the tunnel.

   host1(config-dest-profile)#**tunnel source 1.1.1.1**

3. Set the destination address for the tunnel.

   host1(config-dest-profile)#**tunnel destination subnet 10.0.0.0 255.0.0.0**

4. (Optional) Set the maximum transmission unit (MTU) size for the tunnel.

   host1(config-dest-profile)#**tunnel mtu 10240**

5. (Optional) Configure an IP profile with parameters that are used to stack an upper IP interface over a dynamic GRE tunnel.

   host1(config-dest-profile)#**profile ip-kanata**

6. (Optional) Enable error checking across a GRE tunnel.

   host1(config-dest-profile)#**tunnel checksum**

7. (Optional) Enable sequence number generation for a GRE tunnel.

   host1(config-dest-profile)#**tunnel sequence-datagrams**

8. (Optional) Enable IPSec transport mode.

   host1(config-dest-profile)#**enable ipsec-transport**

9. (Optional) Create a multicast VPN tunnel.

   host1(config-dest-profile)#**tunnel mdt profile kanata-mdt**

Creating a Destination Profile for DVMRP Tunnels

To configure a destination profile for dynamic DVMRP tunnels:

1. Configure a destination profile for DVMRP.

   host1(config-dest-profile)#**dvmrp destination profile kanata1 virtual-router vr1**

2. Set the source address for the tunnel.

   host1(config-dest-profile)#**tunnel source 1.1.1.1**

3. Set the destination address for the tunnel.

   host1(config-dest-profile)#**tunnel destination subnet 10.0.0.0 255.0.0.0**

4. (Optional) Set the maximum transmission unit (MTU) size for the tunnel.

   host1(config-dest-profile)#**tunnel mtu 10240**

5. (Optional) Configure an IP profile with parameters that are used to stack an upper IP interface over a dynamic DVMRP tunnel.

   host1(config-dest-profile)#**profile ip-kanata**

6. (Optional) Enable IPSec transport mode.

   host1(config-dest-profile)#**enable ipsec-transport**

7. (Optional) Create a multicast VPN tunnel.

   host1(config-dest-profile)#**tunnel mdt profile kanata-mdt**

dvmrp destination profile

- Use to configure a destination profile for dynamic DVMRP tunnels.
- Use the **any-virtual-router** keyword to create a default destination profile for all virtual routers. There can only be one default destination profile defined in the system.
- Use the **virtual-router** keyword to specify a specific transport virtual router.
- Example

  host1(config)#**dvmrp destination profile kanata1**

- Use the **no** version to delete the destination profile.

enable ipsec-transport

- Use to specify that the router accepts only dynamic IP tunnels protected by an IPSec transport connection.
- This command is supported in the destination profile only when you have installed an ISM on ERX routers.
- Example

  host1(config-dest-profile)#**enable ipsec-transport**

- Use the **no** version to disable IPSec transport mode.

gre destination profile

- Use to configure a destination profile for dynamic GRE tunnels.
- Use the **any-virtual-router** keyword to create a default destination profile for all virtual routers. There can only be one default destination profile defined in the system.
- Use the **virtual-router** keyword to specify a specific transport virtual router.
- Example

  host1(config)#**gre destination profile kanata2**

- Use the **no** version to delete the destination profile.

profile

- Use to assign an IP profile with parameters that are used to stack an upper IP interface over a dynamic GRE or DVMRP tunnel to the destination profile.
- Example

  host1(config-dest-profile)#**profile ip-kanata**

- Use the **no** version to remove the profile assignment from the destination profile.

tunnel checksum

- Use to enable checksum computation across a GRE tunnel.
- Checksum computation is not supported for DVMRP tunnels.
- Selecting this feature causes the E-series router to drop corrupted packets it receives on the tunnel interface.
- Example

  host1(config-dest-profile)#**tunnel checksum**

- Use the **no** version to disable the checksum option.

tunnel destination

- Use to configure the remote end of the tunnel.
- Specify the IP address of an interface on the remote router or the range of destination addresses:
  - Use the **subnet** keyword to configure the IP address for the destination interface and the mask.
  - Use the **range** keyword to configure the first IP address and the last IP address of the destination interface range
- Example 1—Specifies an IP address and mask for the destination interface

  host1(config-dest-profile)#**tunnel destination subnet 192.13.7.1 255.0.0.0**

- Example 2—Specifies a range of IP addresses for the destination interface

  host1(config-dest-profile)#**tunnel destination range 192.13.7.1 192.13.7.20**

- Use the **no** version to remove the destination of a tunnel.

tunnel mdt profile

- Use to enable multicast distribution tree operation so the IP tunnel component can create an MDT interface.
- The command defines an IP profile with parameters that are used to stack an upper IP interface over a dynamic GRE or DVMRP tunnel.
- Example

  host1(config-dest-profile)#**tunnel mdt profile kanata-mdt**

- Use the **no** version to disable MDT on the interface.

tunnel sequence-datagrams

- Use to enable GRE sequence numbers.
- Specify GRE sequence numbers at both ends of the GRE tunnel.
- Example

  host1(config-dest-profile)#**tunnel sequence-datagrams**

- Use the **no** version to disable sequence numbers.

tunnel source

- Use to configure the source of the tunnel.
- Specify either the primary IP address or the type and specifier of an interface. Do not specify an unnumbered interface.
- You can configure multiple sources in a GRE destination profile or a DVMRP destination profile.
- Example

  host1(config-dest-profile)#**tunnel source 11.11.11.11**

- Use the **no** version to remove the source of a tunnel.

Monitoring Dynamic IP Tunnels

You can monitor dynamic DVMRP and GRE tunnels by using the following commands.

show dvmrp destination profile

- Use to display the configuration of DVMRP destination profiles.
- Field descriptions
  - default dvmrp destination profile—Name of the modified default destination profile on the system
  - dvmrp destination profile—Name of the DVMRP destination profiles configured on the system
  - tunnel checksum—Status of tunnel checksum configuration; enabled or disabled
  - tunnel sequence-datagrams—Status of tunnel sequence datagrams configuration; enabled or disabled
  - tunnel mtu—Value of the tunnel MTU
  - ipsec transport mode—Status of IPSec transport mode configuration; enabled or disabled
  - tunnel mdt—Status of IPSec transport mode configuration; enabled or disabled
  - profile—Name of the profile assigned for upper IP interfaces
  - virtual router—Name of the transport virtual router assigned to the destination profile
  - tunnel destination subnet—Value of the configured destination address subnet
  - tunnel source—Value of the configured source address
- Example 1—Displays all destination profiles configured on the system

```
host1#show dvmrp destination profile
default dvmrp destination profile global
dvmrp destination profile kanata1
dvmrp destination profile kanata2

3 dvmrp destination profiles found
the default destination profile is present
```

- Example 2—Displays a specific destination profile

```
host1#show dvmrp destination profile kanata1
dvmrp destination profile kanata1
  tunnel mtu 10240
  ipsec transport mode disabled
  tunnel mdt disabled
  profile disabled
  virtual router vr1
  tunnel destination subnet 10.0.0.0 255.0.0.0
  tunnel source 1.1.1.1
  tunnel source 1.1.1.2
  tunnel source 1.1.1.3
```

show dvmrp tunnel

- Use to display information about DVMRP tunnels.
- To view detailed information about tunnels, specify the **detail** keyword.
- To view the number of tunnels in a specific state, specify the **state** keyword and the state of the tunnel (disabled, down, enabled, lower-down, not-present, up).
- To view the state of a specific tunnel, specify a tunnel name.
- To view the number of tunnels associated with that IP address, specify an IP address.
- To view the number of tunnels associated with an IP address on the virtual router, specify an IP address with the **virtual-router** keyword and the name of the virtual router.
- Field descriptions
  - DVMRP tunnel—Name and state of the dynamic DVMRP tunnel:
    - Up—Tunnel is operational
    - Down—Tunnel is not operational
    - not-present—Tunnel is not operational, because the hardware (such as a line module) supporting the tunnel is inaccessible
  - Application—Name of the application that created the tunnel
  - Tunnel mtu—Value of the maximum transmission unit for the tunnel
  - Tunnel source address—IP address of the source of the tunnel
  - Tunnel destination address—IP address of the destination of the tunnel
  - Tunnel transport virtual router—Name of the virtual router associated with the tunnel
  - Tunnel mdt—Tunnel MDT state
  - Tunnel checksum option—State of the checksum feature: enabled or disabled
  - Tunnel sequence number option—State of the sequence number feature; enabled or disabled
  - Tunnel up/down trap is enabled—Indicates whether or not the E-series router sends traps to SNMP when the operational state of the tunnels changes

- Tunnel server location—Location of the tunnel server in *slot/port* format (ERX-7xx models, ERX-14xx models, and the ERX-310 router) or *slot/adapter/port* format (E120 and E320 routers).
- Tunnel secured by ipsec transport interface—IPSec interface that secures the tunnel.
- Tunnel administrative state—Configured state of the tunnel: Up or Down
- Statistics—Details of packets received or transmitted by the tunnel
- packets—Number of packets received or transmitted by the tunnel
- octets—Number of octets received or transmitted by the tunnel
- discards—Number of packets not accepted by the tunnel
- Errors—Number of packets with errors received or transmitted by the tunnel
- Data rx—Received data
- Data tx—Transmitted data
- DVMRP tunnels found—Total number of DVMRP tunnels found
- Tunnels were created dynamic—Number of tunnels created dynamically

- Example 1—Displays three dynamic DVMRP tunnels

```
host1:vr11#show dvmrp tunnel
DVMRP tunnel mvpn-dynamic-1 is Up
DVMRP tunnel mvpn-dynamic-2 is Up
DVMRP tunnel mvpn-dynamic-3 is Down

3 DVMRP tunnels found
3 tunnels were created dynamic
```

- Example 2—Displays the detail of a dynamically created DVMRP tunnel for the data MDT application

```
host1:vr11#show dvmrp tunnel detail mvpn-dynamic-1
DVMRP tunnel mvpn-dynamic-1 is Up
tunnel is dynamic
Application is MVPN
Tunnel operational configuration
  Tunnel mtu is '5000'
  Tunnel source address is '1.1.1.1'
  Tunnel destination address is '2.2.2.2'
  Tunnel transport virtual router is vr1
  Tunnel mdt is disabled
  Tunnel up/down trap is enabled
  Tunnel-server location is 4/0
  Tunnel administrative state is Up
Statistics    packets             octets              discards   errors
  Data rx     0                   0                   0          0
  Data tx     0                   0                   0          0

1 DVMRP tunnel found
1 tunnel was created dynamically
```

- Example 3—Displays the detail of a dynamically created DVMRP tunnel for the Mobile IP application

```
host1:vr12#show dvmrp tunnel detail mobileIp-dynamic-1
DVMRP tunnel mobileIp-dynamic-1 is Up
```

```
tunnel is dynamic
Application is Mobile-IP
Tunnel operational configuration
  Tunnel mtu is '5000'
  Tunnel source address is '6.6.6.6'
  Tunnel destination address is '3.3.3.3'
  Tunnel transport virtual router is vr1
  Tunnel mdt is disabled
  Tunnel checksum option is disabled
  Tunnel sequence number option is disabled
  Tunnel key is disabled
  Tunnel up/down trap is enabled
  Tunnel-server location is 6/0
  Tunnel administrative state is Up
Statistics    packets             octets              discards   errors
  Data rx     0                   0                   0          0
  Data tx     0                   0                   0          0
```

show dvmrp tunnel summary

- Use to display a summary of information about DVMRP tunnels.
- Field descriptions
  - Administrative status
    - enabled—Tunnel is available for use
    - disabled—Tunnel is not available for use
  - Operational status
    - up—Tunnel is operational
    - down—Tunnel is not operational
    - not-present—Tunnel is not operational, because the hardware (such as a line module) supporting the tunnel is inaccessible
- Example

```
host1#show dvmrp tunnel summary
Administrative status   enabled   disabled
                        1         0
Operational status      up        down     not-present
                        1         0        0
```

show gre destination profile

- Use to display the configuration of GRE destination profiles.
- Field descriptions
  - default gre destination profile—Name of the modified default destination profile on the system
  - gre destination profile—Name of the GRE destination profiles configured on the system
  - tunnel checksum—Status of tunnel checksum configuration; enabled or disabled
  - tunnel sequence-datagrams—Status of tunnel sequence datagrams configuration; enabled or disabled
  - tunnel mtu—Value of the tunnel MTU

  - ipsec transport mode—Status of IPSec transport mode configuration; enabled or disabled
  - tunnel mdt—Status of IPSec transport mode configuration; enabled or disabled
  - profile—Name of the profile assigned for upper IP interfaces
  - virtual router—Name of the transport virtual router assigned to the destination profile
  - tunnel destination subnet—Value of the configured destination address subnet
  - tunnel source—Value of the configured source address

- Example 1—Displays all GRE destination profiles configured on the system

```
host1#show gre destination profile
default gre destination profile global
gre destination profile boston1
gre destination profile boston2

3 gre destination profiles found
the default destination profile is present
```

- Example 2—Displays a specific GRE destination profile used for dynamic IP tunnel creation

```
host1#show gre destination profile boston1
gre destination profile boston1
  tunnel checksum disabled
  tunnel sequence-datagrams disabled
  tunnel mtu 10240
  ipsec transport mode disabled
  tunnel mdt disabled
  profile kanata
  virtual router vr1
  tunnel destination subnet 10.0.0.0 255.0.0.0
  tunnel source 1.1.1.1
  tunnel source 1.1.1.2
  tunnel source 1.1.1.3
```

- Example 3—Displays a specific GRE destination profile used in a MVPN

```
host1#show gre destination profile boston2
gre destination profile boston2
  tunnel checksum disabled
  tunnel sequence-datagrams disabled
  tunnel mtu 10240
  ipsec transport mode disabled
  tunnel mdt profile kanata-mdt
  profile kanata
  virtual router vr2
  tunnel destination subnet 224.0.0.0 255.0.0.0
  tunnel source 1.1.1.1
  tunnel source 1.1.1.2
  tunnel source 1.1.1.3
```

show gre tunnel

- Use to display information about a GRE tunnel or a list of GRE tunnels.
- To view detailed information about tunnels, specify the **detail** keyword.
- To view the number of tunnels in a specific state, specify the **state** keyword and the state of the tunnel (disabled, down, enabled, lower-down, not-present, up).
- To view the state of a specific tunnel, specify a tunnel name.
- To view the number of tunnels associated with an IP address, specify an IP address.
- To view the number of tunnels associated with an IP address on the virtual router, specify an IP address with the **virtual-router** keyword and the name of the virtual router.
- Field descriptions
  - GRE tunnel—Name and state of the dynamic GRE tunnel:
    - Up—Tunnel is operational
    - Down—Tunnel is not operational
    - not-present—Tunnel is not operational, because the hardware (such as a line module) supporting the tunnel is inaccessible
  - Application—Name of the application that created the tunnel
  - Tunnel mtu—Value of the maximum transmission unit for the tunnel
  - Tunnel source address—IP address of the source of the tunnel
  - Tunnel destination address—IP address of the destination of the tunnel
  - Tunnel transport virtual router—Name of the virtual router associated with the tunnel
  - Tunnel mdt—State of the tunnel MDT
  - Tunnel checksum option—State of the checksum feature: enabled or disabled
  - Tunnel sequence number option—State of the sequence number feature; enabled or disabled
  - Tunnel up/down trap—Indicates whether or not the E-series router sends traps to SNMP when the operational state of the tunnels changes, enabled or disabled
  - Tunnel server location—Location of the tunnel server in *slot/port* format (ERX-7xx models, ERX-14xx models, and the ERX-310 router) or *slot/adapter/port* format (E120 and E320 routers).
  - Tunnel is secured by ipsec transport interface—IPSec interface that secures the tunnel.
  - Tunnel administrative state—Configured state of the tunnel: up or down
  - Statistics—Details of packets received or transmitted by the tunnel
  - packets—Number of packets received or transmitted by the tunnel
  - octets—Number of octets received or transmitted by the tunnel
  - discards—Number of packets not accepted by the tunnel

- Errors—Number of packets with errors received or transmitted by the tunnel
- Data rx—Received data
- Data tx—Transmitted data
- Tunnels found—Total number of GRE tunnels found
- Tunnels were created dynamic—Number of tunnels created dynamically

- Example 1—Displays three dynamic GRE tunnels

```
host1:vr11#show gre tunnel
GRE tunnel mobileIp-dynamic-1 is Up
GRE tunnel mvpn-dynamic-2 is Up
GRE tunnel mvpn-dynamic-3 is Down

3 GRE tunnels found
3 tunnels were created dynamic
```

- Example 2—Displays the detail of a dynamically created GRE tunnel for the data MDT application

```
host1:vr11#show dvmrp tunnel detail mvpn-dynamic-1
GRE tunnel mvpn-dynamic-1 is Up
tunnel is dynamic
Application is MVPN
Tunnel operational configuration
  Tunnel mtu is '5000'
  Tunnel source address is '1.1.1.1'
  Tunnel destination address is '2.2.2.2'
  Tunnel transport virtual router is vr1
  Tunnel mdt is disabled
  Tunnel checksum option is disabled
  Tunnel sequence number option is disabled
  Tunnel up/down trap is enabled
  Tunnel-server location is 4/0
  Tunnel administrative state is Up
Statistics    packets             octets              discards   errors
  Data rx     0                   0                   0          0
  Data tx     0                   0                   0          0

1 GRE tunnel found
1 tunnel was created dynamically
```

- Example 3—Displays the detail of a dynamically created GRE tunnel for the Mobile IP application

```
host1:vr12#show gre tunnel detail mobileIp-dynamic-1
GRE tunnel mobileIp-dynamic-1 is Up
tunnel is dynamic
Application is Mobile-IP
Tunnel operational configuration
  Tunnel mtu is '5000'
  Tunnel source address is '6.6.6.6'
  Tunnel destination address is '3.3.3.3'
  Tunnel transport virtual router is vr1
  Tunnel mdt is disabled
  Tunnel checksum option is disabled
  Tunnel sequence number option is disabled
  Tunnel key is disabled
  Tunnel up/down trap is enabled
  Tunnel-server location is 6/0
  Tunnel administrative state is Up
```

```
Statistics    packets              octets               discards   errors
  Data rx     0                    0                    0          0
  Data tx     0                    0                    0          0
```

show gre tunnel summary

- Use to display a summary of information about GRE tunnels.
- Field descriptions
  - Administrative status
    - enabled—Tunnel is available for use
    - disabled—Tunnel is not available for use
  - Operational status
    - up—Tunnel is operational
    - down—Tunnel is not operational
    - not-present—Tunnel is not operational, because the hardware (such as a line module) supporting the tunnel is inaccessible
- Example

```
host1#show gre tunnel summary
Administrative status    enabled    disabled
                         3          0
Operational status       up         down       not-present
                         3          0          0
```